Requested Patent: JP2002312205A

Title:

SAVING PROCESSING METHOD FOR ACCESS LOG INFORMATION, SAVING PROCESSING DEVICE FOR THE SAME AND PROCESSING PROGRAM FOR THE SAME ;

Abstracted Patent: JP2002312205 ;

Publication Date: 2002-10-25 ;

Inventor(s): ISE MASAHIRO ;

Applicant(s): HITACHI INFORMATION SYSTEMS LTD ;

Application Number: JP20010112116 20010411 ;

Priority Number(s): ;

IPC Classification: G06F11/34; G06F11/30 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a saving processing method for access log information surely saving access log information indicating access to a PC or resource thereof which is useful for analysis of abnormality which suddenly occurs in the PC.SOLUTION: A log monitor part 130 acquires log information composed of information of system condition of the PC and an error determining processing part 140 determines if the log information is error information or not. If the log information is error information, an access log read processing part 150 acquires access log information corresponding to a designated duration closest to a point of error log information occurrence and a designated accumulation capacity closest to the point of error log information occurrence with referring access log type indicating a type of PC access information corresponding to the log information based on information given from a parameter file 102, and the access log saving processing part 170 saves the access log information in another file.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312205
（P2002－312205A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.'	識別記号	Ｆ１	テーマコード'(参考)
Ｇ０６Ｆ　11/34		Ｇ０６Ｆ　11/34	Ｈ　５Ｂ０４２
11/30		11/30	Ｋ

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願2001－112116(P2001－112116)

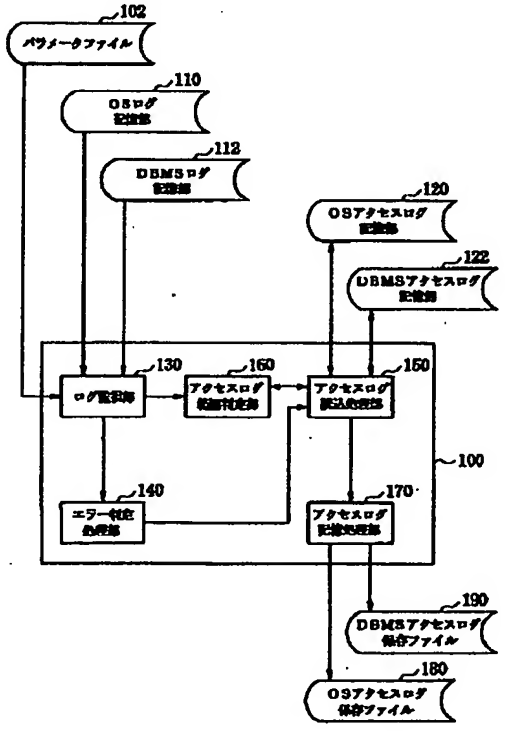
(22)出願日　平成13年４月11日(2001.4.11)

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　伊勢　正浩
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

Ｆターム(参考)　5B042 GC08 HH30 KK15 LA20 MA08 MB05 MC15 MC36 MC40

(54)【発明の名称】　アクセスログ情報の保存処理方法とその保存処理装置およびその処理プログラム

(57)【要約】
【課題】　ＰＣにおいて突然発生する異常に対して、その異常発生の解析に有用である、そのＰＣまたはその資源にアクセスしたアクセスログ情報を、確実に保存するアクセスログ情報の保存処理方法を提供すること。
【解決手段】　ＰＣのシステム状況の情報からなるログ情報をログ監視部１３０で取得し、そのログ情報がエラー情報であるか否かをエラー判定処理部１４０で判定し、そのログ情報がエラー情報であれば、アクセスログ読込処理部１５０は、パラメータファイル１０２から得た情報を基に、そのログ情報に対応する、ＰＣへのアクセス情報の種別を示すアクセスログ種別を参照し、エラーのログ情報の発生した時点の直近の所定期間、またはエラーのログ情報の発生した時点の直近の所定累積容量に、それぞれ対応したアクセスログ情報を取得し、アクセスログ記憶処理部１７０により別のファイルに記憶し保存することを特徴とする。



【特許請求の範囲】
【請求項１】　コンピュータのエラー情報を含むシステム状況の情報からなるログ情報を取得し、
前記ログ情報が、エラー情報であるか否かを判定し、
該ログ情報がエラー情報であると判定された場合、該ログ情報を基に、エラー種別ファイル内の該ログ情報に対応する、前記コンピュータへのアクセス情報の種別を示すアクセスログ種別を参照し、該アクセスログ種別に対応したファイルを選択し、
該ログ情報の発生した時点の直近の所定期間内に発生した前記アクセス情報からなるアクセスログ情報、または該ログ情報の発生した時点の直近に発生した前記アクセス情報からなるアクセスログ情報の内でその累積容量が所定容量以下となるアクセスログ情報を取得し、前記ファイルに記憶することを特徴とするアクセスログ情報の保存処理方法。
【請求項２】　コンピュータのエラー情報を含むシステム状況の情報からなるログ情報を監視し取得するログ監視部と、
前記ログ監視部が取得した前記ログ情報が、エラー情報であるか否かを判定するエラー判別処理部と、
前記エラー判別処理部により、該ログ情報がエラー情報であると判定された場合、該ログ情報を基に、エラー種別ファイル内の該ログ情報に対応する、前記コンピュータへのアクセス情報の種別を示すアクセスログ種別を参照し、該アクセスログ種別に対応したファイルを選択し、該ログ情報の発生した時点の直近の所定期間内に発生した前記アクセス情報からなるアクセスログ情報、または該ログ情報の発生した時点の直近に発生した前記アクセス情報からなるアクセスログ情報の内でその累積容量が所定容量以下となるアクセスログ情報を取得するログ情報読込処理部と、
前記ログ情報読込処理部からの該アクセスログ情報を、前記ファイルに記憶するアクセスログ情報記憶処理部とを有することを特徴とするアクセスログ情報の保存処理装置。
【請求項３】　請求項１に記載のアクセスログ情報の保存処理方法における各処理を、コンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータの障害解析を行う際に有用なアクセスログ情報の保存処理方法に関し、特に、エラーについてのログ情報が発生した時点で、対応するアクセスログ情報を抽出し、別のファイルに保存し上記障害解析に役立てるアクセスログ情報の保存処理方法とその保存処理装置およびその処理プログラムに関する。
【０００２】
【従来の技術】コンピュータ（以下、ＰＣという）、あるいはネットワークに接続された端末ＰＣやサーバＰＣでは、エラー情報やシステム等の状況を記録するログ情報と、ＰＣやＰＣの資源へのアクセス情報を記録するアクセスログ情報がある。ログ情報は常時記録されているが、ＰＣやＰＣの資源へのアクセスログ情報は、情報量が膨大になるため取得されないか、あるいは古いアクセスログ情報を随時切り捨ててファイル容量が増加しないような処理を行いアクセスログ情報を保存している。特開平１１－９６０４６号公報（以下、文献１）には、ＰＣの実行で問題があった時に、課題を予め指定し、特定の情報を収集する方法が示されている。特開平４－１６２１５３号公報（以下、文献２）には、障害発生時の障害要因に応じ、メモリ内に記録された障害情報の内容を収拾選択決定する内容が示されている。
【０００３】
【発明が解決しようとする課題】ＰＣ上で異常が発生した時には、ログ上で異常発生の内容を調査した上で、具体的には、異常が発生した資源へのアクセスログ情報を調べることによって、異常発生の原因を究明することを容易にする。しかし、すべてのアクセスログ情報を保存しておけば膨大なファイル容量を必要とすることになる。通常、アクセスログ情報は１分間に１ＭＢ以上のログ情報が発生し、多い場合は１分間に数ＭＢ以上のアクセスログ情報が発生する。このため、アクセスログ情報を収集・保存することはあまりない。また、アクセスログ情報の古い情報を切り捨てるようにすると、異常発生に気が付かなかった場合、またはアクセスログ情報収集操作開始までに時間がかかってしまった場合に、異常が発生した時点のアクセスログ情報が消滅してしまう可能性がある。特に、遠隔地にあるＰＣにおいて、オンラインで接続されていなく、障害の対応に不慣れな操作員しかいない場合、異常発生時のアクセスログ情報が消失してしまう。これらのことによって、異常が発生した時点のアクセスログ情報が消失することで、異常発生の原因究明が困難になってしまうことがあった。
【０００４】また、上記従来技術の文献１にあるように、あらかじめ問題点が判明している障害には対応できる技術は存在するが、突然発生する障害には対応できない。突然発生する障害は、再現性がないことが多く、これらの問題を解決するためには、情報を常に必要な分だけ取得・保存しておく必要がある。また、上記文献２にあるように、その時点でのＰＣの状態だけを記録しただけでは、障害の解決に至ることは難しい。
【０００５】本発明の目的は、上述の課題に鑑みてなされ、ＰＣにおいて突然発生する異常に対して、異常発生時に、その時点の前までにＰＣまたはその資源にアクセスしたアクセスログ情報を確実に保存することで、異常発生の原因究明を容易にすることができるアクセスログ情報の保存処理方法とその保存処理装置およびその処理プログラムを提供することにある。

【0006】
【課題を解決するための手段】上記目的を達成するために、本発明に係るアクセスログ情報の保存処理方法では、コンピュータのエラー情報を含むシステム状況の情報からなるログ情報を取得し、このログ情報が、エラー情報であるか否かを判定し、そのログ情報がエラー情報であると判定された場合、そのログ情報を基に、エラー種別ファイル内のログ情報に対応する、コンピュータへのアクセス情報の種別を示すアクセスログ種別を参照し、このアクセスログ種別に対応したファイルを選択し、エラー情報のログ情報の発生した時点の直近の所定期間内に発生したアクセス情報からなるアクセスログ情報、またはエラー情報のログ情報の発生した時点の直近に発生したアクセス情報からなるアクセスログ情報の内でその累積容量が所定容量以下のアクセスログ情報を取得し、選択したファイルに記憶することを特徴とする。こうすることで、ログ情報に異常情報が発生した時点の前の一定期間のアクセスログ情報を、本来のアクセスログ情報の保存ファイルとは別のファイルに保存できるようになり、異常解決のために有用な情報であるアクセスログ情報の消失を防止できるようになる。
【0007】
【発明の実施の形態】以下、本発明の実施の形態を、図1～図4を用いて詳細に説明する。図1は、本発明に係るアクセスログ情報の保存処理装置100の構成例を示す図である。図2は、図1の保存処理装置100を用いたアクセスログ情報の保存処理を示すフローチャートである。図3は、図1のパラメータファイル102の構成例を示す図である。図4は、記録されるログ情報の内容例を示す図である。
【0008】図1に示すアクセスログ情報の保存処理装置100は、ログ監視部130、エラー判定処理部140、アクセスログ読込処理部150、アクセスログ範囲判定処理部160、およびアクセスログ記憶処理部170を有して構成されている。また、保存処理装置100の外部には、パラメータファイル102、OSログ記憶部110、DBMSログ記憶部112、OSアクセスログ記憶部120、DBMSアクセスログ記憶部122、OSアクセスログ保存ファイル180、およびDBMSアクセスログ保存ファイル190を有している。なお、OSはオペレーティングシステムであり、DBMSはデータベース管理システムの略である。
【0009】ここで、パラメータファイル102は、例えば図3に示すようなテーブル上に、ログ種別301、アクセスログ種別302、切出種別303、切出範囲304、および保存ファイル305の各項目を有して構成されているファイルである。ログ種別301は、コンピュータ（以下、PCという）のシステム状況情報などのログ情報に対して、そのログ情報を種類別に分類した項目である。アクセスログ種別302は、PCへのアクセス情報や、WebサーバPCの動作を記録したアクセスログ情報を種類別に分類した項目である。切出種別303は、特定のアクセスログ情報のみをコピーする際に、そのコピー条件となる種別を設定した項目である。切出範囲304は、切出種別303で設定した条件に基づいて、その特定のアクセスログ情報をコピーする範囲を設定した項目である。保存ディレクトリ305は、コピー選択した特定のアクセスログ情報を記録したファイルを保存する、保存先となるディレクトリを設定した項目である。
【0010】OSログ記憶部110はOSのログ情報を、DBMSログ記憶部112はDBMSのログ情報を記憶する。OSアクセスログ記憶部120はOSへのアクセスログ情報を、DBMSアクセスログ記憶部122はDBMSへのアクセスログ情報を記憶する。OSアクセスログ保存ファイル180、およびDBMSアクセスログ保存ファイル190は、共に、上述したパラメータファイル102の保存ディレクトリ305項目で設定された保存ディレクトリに存在している。
【0011】ログ監視部130は、主に、指定されたログを随時監視し、ログ情報が発生する毎にその内容を読み込む機能を有する。エラー判定処理部140は、読み込まれたログ情報がエラー情報であるか否かを判定する。アクセスログ読込処理部150は、読み込まれたエラー情報の内容に対応するパラメータファイル102の設定情報が記憶されたアクセスログ範囲判定処理部160に基づいて、OSアクセスログ記憶部120またはDBMSアクセスログ記憶部122内の特定のアクセスログ情報を選択する。アクセスログ記憶処理部170は、この選択し取得したアクセスログ情報を所定のディレクトリの所定のファイルに保存する。
【0012】さて、通常、ログ情報は図4に示すように、一般の情報メッセージとエラーメッセージとが混在した状態で記録される。本発明では、エラーが発生した時において、そのエラーに対応するアクセスログ情報を別に保存することで、そのエラーの原因となる障害の解析に役立てるという効果を奏することができるようになる。
【0013】以下に、図2のフローチャートを用いて、アクセスログ情報の記憶処理装置100の動作を説明する。
【0014】ログ監視部130は、起動時において、パラメータファイル102を読み込み、アクセスログ範囲判定部160にその情報を記憶する（ステップS201）。ログ監視部130は、パラメータファイル102で設定されている監視対象となるログ情報である、OSログ記憶部110およびDBMSログ記憶部112を随時監視し、そのログ情報が書き込まれる毎に、そのログ情報を取得する（ステップS202）。
【0015】エラー判定処理部140は、その取得した

ログ情報がエラー情報であるのか否かを判定する（ステップＳ２０３）。エラー情報でない場合は、ステップＳ２０２に戻り、引き続きログ監視部１３０がログ情報を監視する。エラー情報である場合は、アクセスログ判定処理部１６０に記憶されたログ種別３０１に対応するアクセスログ種別３０２を基に、該当するアクセスログ情報が記憶されたファイルを選択する（ステップＳ２０４）。これと同時に、アクセスログ範囲判定部１６０は、切出種別３０３および切出範囲３０４を読み込み、例えば、その切出種別３０３が「期間」であった場合には（ステップＳ２０５）、そのエラーログ情報に記載された時刻から切出範囲３０４に設定された期間を引いた時刻を計算し、特定の期間を算出する。

【００１６】そして、アクセスログ読込処理部１５０は、対象となるＯＳアクセスログ記憶部１２０またはＤＢＭＳアクセスログ記憶部１２２を参照し、この特定の期間内におけるアクセスログ情報を選択し取得する（ステップＳ２０６）。なお、ステップＳ２０５において、切出種別３０３が「容量」であった場合には、そのエラーログ情報を取得した時点において、アクセスログ読込処理部１５０は、対象となるＯＳアクセスログ記憶部１２０またはＤＢＭＳアクセスログ記憶部１２２を参照し、最新のアクセスログ情報から積算してその容量に相当する分のアクセスログ情報を選択し取得する（ステップＳ２０７）。

【００１７】この後、アクセスログ記憶処理部１７０は、既に存在するファイルに取得したアクセスログ情報が上書きされることがないように、例えば、時刻を含めるなどしたユニークなファイル名を有するファイルを生成する（ステップＳ２０８）。アクセスログ記憶処理部１７０は、このファイルに先に取得したアクセスログ情報を、アクセスログ範囲判定部１６０に記憶された保存ディレクトリ３０５で指定されたディレクトリに保存する（ステップＳ２０９）。

【００１８】こうすることで、ログ情報に異常情報が発生した時点の前の一定期間のアクセスログ情報を、本来のアクセスログ情報の保存ファイルとは別のファイルに保存できるようになり、異常解決のために有用な情報であるアクセスログ情報の消失を防止できるようになる。

【００１９】なお、本発明は、図１～図４を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々の変更が可能である。

【００２０】例えば、本実施形態では、エラーが発生する毎に新規なファイルを作成し、図３のパラメータファイルの保存ディレクトリ３０５項目における指定のディレクトリに、そのファイルを保存することを想定したが、図３のパラメータファイルの保存ディレクトリ３０５項目の代わりに、保存ファイルを直接指定し、そのファイルにアクセスログ情報を蓄積保存してもよい。

【００２１】また、本実施形態では、障害解析に役立てる観点から、エラーの発生した前のアクセスログ情報を保存するようにしていたが、例えば、エラーが発生した前後のアクセスログ情報を保存するようにしてもよい。

【００２２】また、本実施形態では、特に、ＯＳとＤＢＭＳとのログ情報にエラーが生じた場合についてのみ取り上げ説明したが、他に、サーバ機能を有するＰＣにおいて、エラーが生じたネットワークログ情報に対するアクセスログ情報を保存し、その障害解析に役立てるようにしてもよい。

【００２３】また、上述の実施形態において、その処理を行う各プログラムをアプリケーションソフトとして、ハードディスク等の記録媒体に格納しておいてもよい。このようにすれば、ＣＤ－ＲＯＭ等の可搬型記録媒体にプログラム等を格納して売買したり、携帯することができるようになる。

【００２４】

【発明の効果】本発明では、ログ情報に異常情報が発生した時点の前後の一定期間のアクセスログ情報を、本来のアクセスログ情報の保存ファイルとは別のファイルに保存できるようになり、異常解決のために有用な情報であるアクセスログ情報の消失を防止できるようになる。

【図面の簡単な説明】

【図１】本発明に係るアクセスログ情報の保存処理装置１００の構成例を示す図である。

【図２】図１の保存処理装置１００を用いたアクセスログ情報の保存処理を示すフローチャートである。

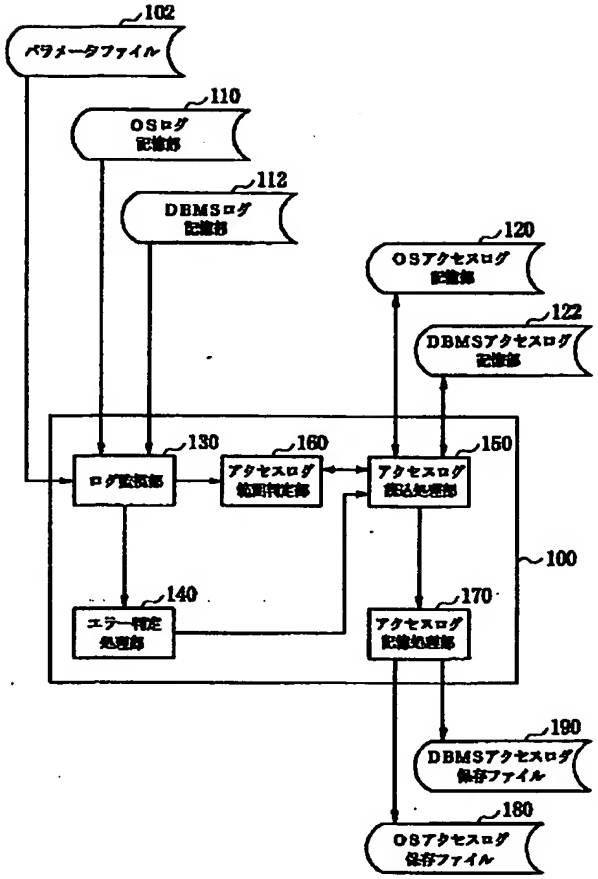
【図３】図１のパラメータファイル１０２の構成例を示す図である。

【図４】記録されるログ情報の内容例を示す図である。

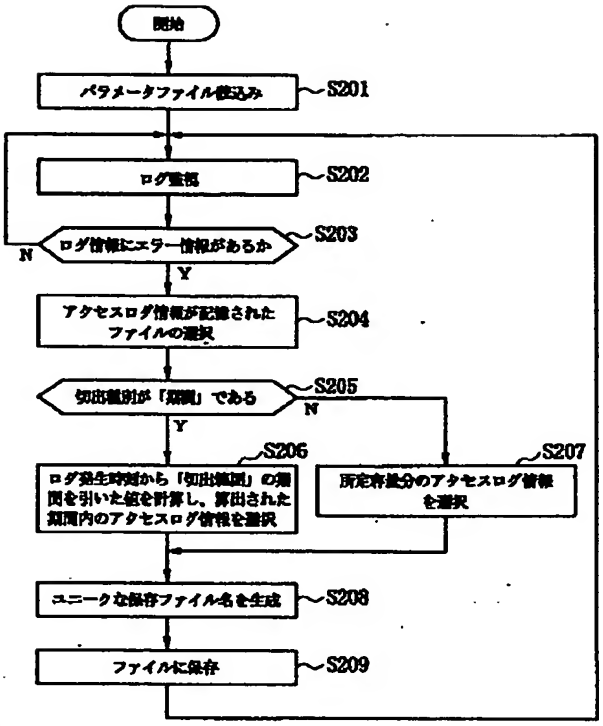
【符号の説明】

１００：保存処理装置
１０２：パラメータファイル
１１０：ＯＳログ記憶部
１１２：ＤＢＭＳログ記憶部
１２０：ＯＳアクセスログ記憶部
１２２：ＤＢＭＳアクセスログ記憶部
１３０：ログ監視部
１４０：エラー判定処理部
１５０：アクセスログ読込処理部
１６０：アクセスログ範囲判定部
１７０：アクセスログ記憶処理部
１８０：ＯＳアクセスログ保存ファイル
１９０：ＤＢＭＳアクセスログ保存ファイル

【図1】



【図2】



【図3】

102

301 ログ種別	302 アクセスログ種別	303 切出種別	304 切出範囲	305 保存ディレクトリ
OSログ	OSアクセスログ	期間	5分間	C:¥LOG¥OS¥
	ディスクアクセスログ	容量	1MB	C:¥LOG¥DISK¥
DBMSログ	DBMSアクセスログ	期間	5分間	C:¥LOG¥DBMS¥

【図4】

12/07/28	23:30:04	RemoteAccess	情報	20159	N/A	接続しましたが、切断されました。
12/07/28	23:29:52	RemoteAccess	情報	20158	N/A	接続を正常に確立しました。
12/07/28	23:26:29	EventLog	情報	6005	N/A	イベント ログ サービスが開始されました。
12/07/28	23:26:29	EventLog	情報	6009	N/A	Microsoft(R)Windows2000(R) 5.0 2195 Uniprocessor Free.
12/07/28	23:26:29	Service Control Manager	エラー	7000	N/A	irDA Protocol サービスは次のエラーのため開始できませんでした。